Campanha de Conscientização Cibernética

PHISHING E OUTROS GOLPES



EXÉRCITO BRASILEIRO



Produção:







NEM TUDO NA INTERNET É CONFIÁVEL, PODE SER GOLPE!

Golpistas estão sempre criando novos **truques** para enganar e tirar **vantagem** das pessoas. Não se deixe enganar.

Desconfie sempre.

Na Internet circulam informações de qualquer tipo e origem, inclusive falsas e maliciosas. Acreditar cegamente em tudo que recebe ou acessa facilita a ação de golpistas.

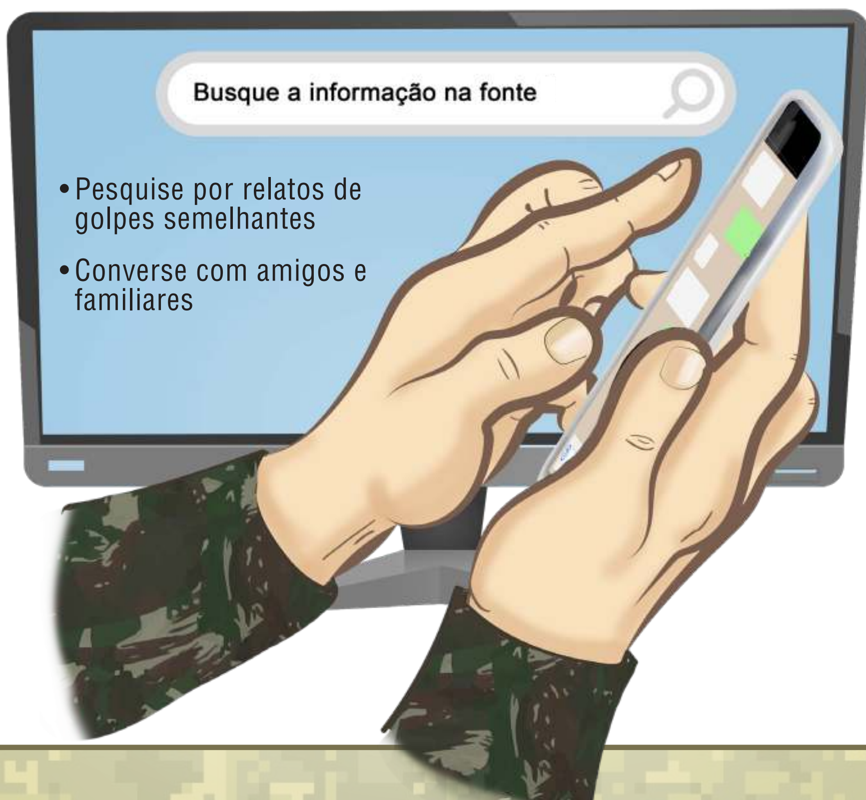


Use senso crítico:

PODE SER UM GOLPE!!

BUSQUE MAIS INFORMAÇÕES

É preciso desconfiar, **manter a calma e checar** se a mensagem que recebeu ou o conteúdo que viu na Internet são confiáveis, para não cair na lábia de golpistas.



FIQUE ATENTO AO TOM DA MENSAGEM

Golpistas exploram os sentimentos das pessoas, como medo, obediência, caridade, carência afetiva e ganância, **para convencê-las a agirem** como eles querem e de forma rápida, **sem pensar**.

Desconfie de mensagens contendo:

» ameaças
» oportunidades de ganho fácil
» promoções ou descontos muito grandes
» pedido de sigilo
» apelo emocional
» senso de urgência



QUESTIONE SE O CONTEÚDO FAZ SENTIDO

Golpistas costumam enviar mensagens em massa com conteúdo genérico **esperando** que alguém **“morda a isca”**.

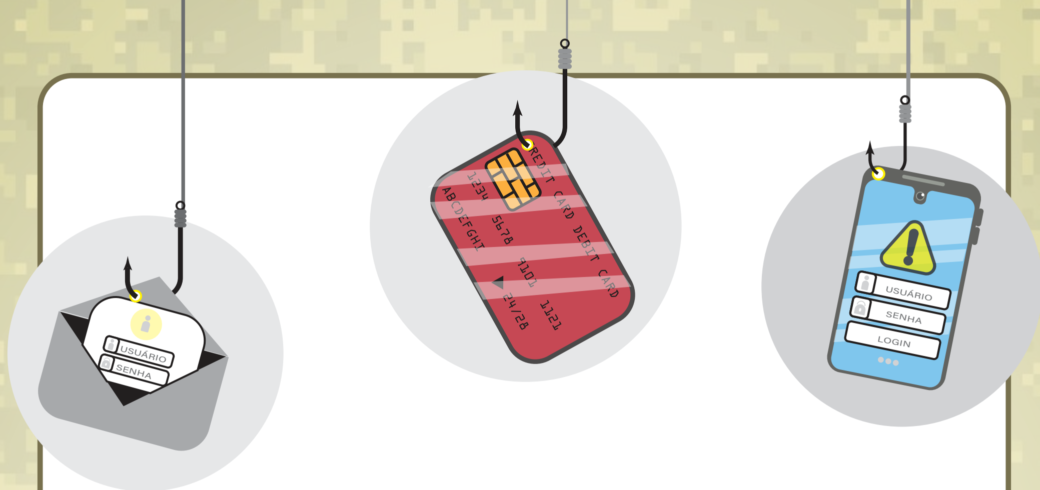
Questionar se o **conteúdo faz sentido para você** ajuda a não cair em golpes.

Sempre pergunte:

- tenho conta neste banco?
- esse é o contato que normalmente uso com esta instituição?
- o valor da cobrança confere?

Observe se há **erros de escrita**.





FIQUE ATENTO A GOLPES DO DIA A DIA

Golpe comum, o ***phishing*** visa **capturar dados** dos usuários. Normalmente é enviado por meio de mensagens eletrônicas com **temas** que **atraem** sua **atenção**, para fazê-lo acessar *links* maliciosos ou instalar determinado *malware*.

Suspeite de mensagens com temas cotidianos, como:

» recadastramento de token
» cancelamento de CPF
» débitos pendentes
» oferta de emprego
» pontos ou bônus a vencer

Não faça o que estão solicitando na mensagem

» na dúvida, contate a instituição usando um canal oficial

Phishing é um tipo de fraude na qual o golpista tenta obter informações pessoais e financeiras do usuário, combinando meios técnicos e engenharia social.

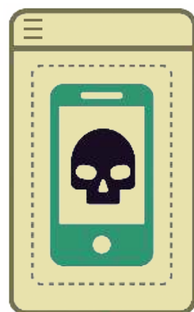
 

A palavra ***Phishing***, do inglês "*fishing*", é uma analogia criada pelos golpistas, em que "iscas" (mensagens eletrônicas) são usadas para "pescar" informações de usuários.



ATENÇÃO TAMBÉM AOS GOLPES DO MOMENTO

Para atrair vítimas, oportunistas exploram temas de destaque no momento, como Imposto de Renda, eleições, Copa do Mundo, promoções como Black Friday e acontecimentos que geram comoção, como desastres e doenças graves.





- **Suspeite** de ofertas muito vantajosas e lembre-se que “quando a esmola é demais, o santo desconfia”
- Busque informações somente em **fontes oficiais**, antes de fazer qualquer pagamento ou doação







NÃO RESPONDA, DENUNCIE

Ao responder uma mensagem você confirma que sua conta está ativa. Pode ainda revelar informações e preferências que ajudam o golpista a ser mais convincente.

» Denuncie mensagens, anúncios e perfis maliciosos
  - use as opções disponibilizadas pelas plataformas

» Bloqueie números de telefone e contas que enviam mensagens maliciosas



NÃO CLIQUE EM TODOS OS *LINKS* QUE RECEBE

Links e códigos QR maliciosos são usados para direcionar usuários para páginas falsas ou com *malware*, a fim de capturar dados e cometer fraudes.

- Antes de clicar, analise o contexto e os detalhes. **NA DÚVIDA, NÃO CLIQUE!**
- **Desconfie** até mesmo de mensagens enviadas por “conhecidos”. Se necessário, contate quem supostamente a enviou, usando outro meio de comunicação
- Só leia códigos QR se tiver certeza que a fonte é **confiável**



MENSAGENS

Parabéns, você GANHOU!!!

Clique no link abaixo para garantir seu PRÊMIO.

CLIQUE AQUI

ACESSE O SITE OU APLICATIVO OFICIAL







Existem muitas páginas falsas e aplicativos maliciosos que tentam se passar por organizações conhecidas, como bancos, comércio eletrônico e redes sociais. É preciso tomar cuidado para **somente** acessar **sites** ou instalar **aplicativos legítimos**.

» Acesse o site digitando o endereço (URL) diretamente no navegador
  - se usar sites de busca, confirme se a URL apresentada é a correta
  - use sempre **conexão segura (https)**

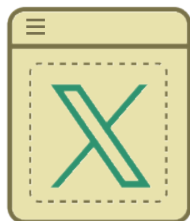
» Instale apenas **aplicativo oficial** da instituição

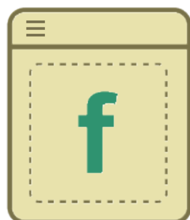




BUSQUE O PERFIL OFICIAL DAS INSTITUIÇÕES NAS REDES SOCIAIS







Ao fazer contato com instituições em redes sociais, como serviços de atendimento ao cliente, é preciso verificar se o perfil é o legítimo, para não entregar seus dados a golpistas, que criam perfis falsos.

- Confira se é o **perfil oficial**
- Procure pelo indicativo de "**conta verificada**", sempre que disponível

REDUZA A QUANTIDADE DE DADOS SOBRE VOCÊ

Quanto mais informações você divulga, mais fácil será furtar sua identidade e mais convincente o golpista será nas abordagens. As informações também podem ser usadas para tentar adivinhar suas senhas.

» Pense bem antes de publicar algo
  - avalie o que publica e quem terá acesso

» Seja seletivo ao aceitar novos contatos



CUIDADOS COM OPERAÇÕES BANCÁRIAS E COMPRAS ONLINE

CONFIRME A IDENTIDADE ANTES DE FAZER TRANSAÇÕES FINANCEIRAS

Golpistas exploram a confiança entre familiares e amigos pedindo empréstimos ou ajuda para pagar contas, geralmente com **urgência**. Eles costumam usar contas invadidas ou alegam alteração de contato, como número de telefone.

» Desconfie de mensagens pedindo **ajuda financeira**
- contate a pessoa por outro meio de comunicação
- informe o ocorrido ao real dono da conta, amigos e familiares

» Confira sempre os **dados do recebedor** antes de efetivar transações



VERIFIQUE SE O SITE OU LOJA É CONFIÁVEL

Golpistas criam sites falsos de comércio eletrônico com preços abaixo do mercado e enganam os clientes, que não recebem as mercadorias. Os dados fornecidos podem ainda ser usados em outras fraudes.

- » Pesquise a reputação da empresa e as opiniões dos clientes
  - em redes sociais e sites de reclamações
  - prefira sites e lojas que você conheça ou tenha boas referências
- » Faça uma pesquisa de mercado e desconfie se o preço estiver muito baixo



NÃO ACEITE INTERMEDIÁRIOS EM TRANSAÇÕES DE COMPRA E VENDA

Fraudadores criam anúncios falsos com valores mais baixos para atrair compradores. Se dizendo intermediários na transação, recebem o dinheiro e não o repassam ao real vendedor, que acaba não fazendo a entrega.

- Conduza toda a transação somente pela plataforma do anúncio
- **Suspeite** de intermediário pedindo sigilo sobre valores da negociação





FAÇA PAGAMENTOS APENAS NA PLATAFORMA OFICIAL DA COMPRA



Fraudadores alegam **falha de sistema** e pedem às vítimas para fazer pagamentos fora da plataforma da compra. No pagamento separado, o valor é alterado e ocultado para cobrar a mais. O cartão também pode ser clonado.

» Ao fazer compras em sites ou aplicativos:
- se usar cartão de crédito, prefira o **cartão virtual**
- não faça pagamentos fora da plataforma

» Ao fazer qualquer pagamento:
- **confira o valor** antes de autorizar a cobrança
- verifique o valor cobrado em sua conta e/ou cartão

FUI VÍTIMA DE GOLPE!!! O QUE DEVO FAZER?





MONITORE SUA VIDA FINANCEIRA E SUA IDENTIDADE

O furto da sua identidade pode causar muitos prejuízos. Você pode ficar com dívidas em seu nome, perder reputação e crédito e ainda se envolver em processos judiciais.

» Ative alertas e monitore extratos de cartões e contas bancárias
» Contate as instituições envolvidas para esclarecer dúvidas ou contestar irregularidades
» Acompanhe seus registros financeiros no Banco Central
  • busque pelo serviço “**Registrato**”



Sinais de furto de identidade:

» notificações de instituições de proteção ao crédito
» contas bancárias, chaves Pix, empréstimos, cartões ou benefícios que não solicitou

FAÇA BOLETIM DE OCORRÊNCIA (BO)

O BO é o registro policial que ajuda você a se defender caso seja vítima de golpe, em especial nos casos de perda financeira e de furto de identidade. É geralmente exigido para contestar fraudes e acionar seguros.



» Registre ocorrência na **autoridade policial** caso:
- alguém esteja se passando por você (furto de identidade)
- tenha prejuízos financeiros

RECUPERE SUAS CONTAS E TROQUE SUAS SENHAS

Contas invadidas podem ser a **porta de entrada** para fraudes. Podem ser usadas para trocar senhas de outras contas, inclusive de instituições financeiras, e para aplicar golpes em seus contatos.

Senha anterior

#########

Nova senha

****

Confirme nova senha

****

» Se alguma conta sua foi invadida:
- tente trocar sua senha
- siga os procedimentos para recuperação do acesso, se necessário

» Denuncie na plataforma se identificar perfil falso em seu nome

» Informe seus contatos



Veja mais dicas na Cartilha

AUTENTICAÇÃO

SAIBA MAIS


Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais fascículos da Campanha de Conscientização Cibernética no site EB.MIL.BR



EXÉRCITO BRASILEIRO

Novos Desafios, Mesmos Valores

Produção:







Fonte:
Cartilha de Segurança para Internet - https://cartilha.cert.br/
Material sob Licença Creative Commons CC BY-NC-ND 4.0
Adaptado com permissão.



cert.br nic.br cgi.br